Algorithms: what every auditor needs to know

Our organisations are increasingly shaped by algorithms; the unseen influence in our lives. Yet how often are they mentioned in the scope of an audit engagement or a final report?

Don't click away…..this is not a technical read! It's for all audit leaders.

Algorithms are part of the digital workforce, an unseen labour force, increasing efficiency by rapidly assimilating and assessing data. But can we trust them? How well do we know them? Who recruited them? What vetting did they go through?

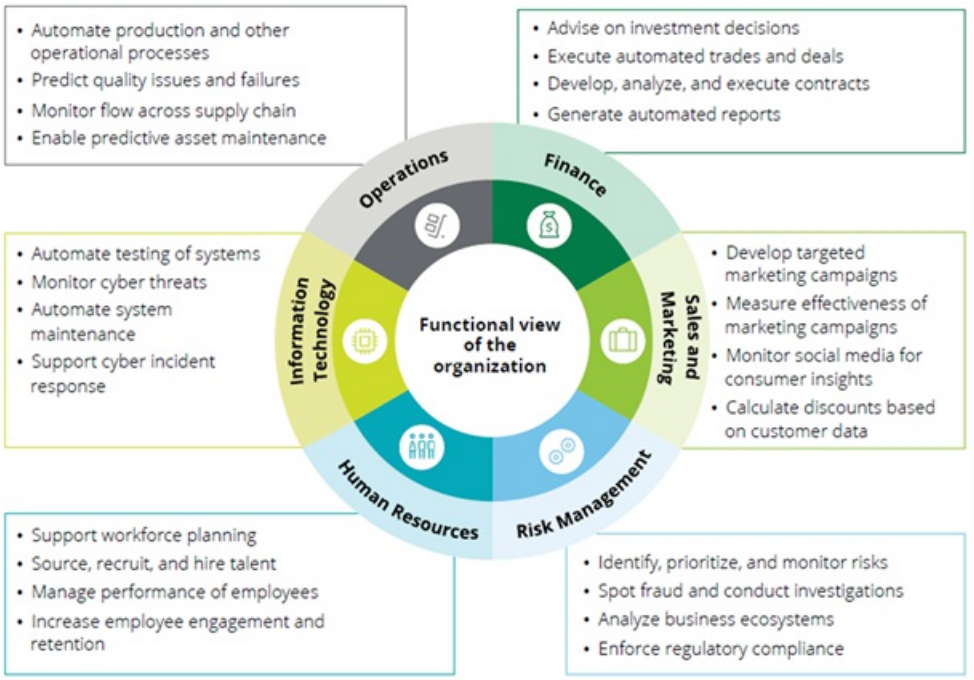
What risks is your organisation exposed to by the algorithms that are used?
Do you know? Does anyone in your organisation know?

What do we mean by algorithms?

Algorithms like most things computer orientated are surrounded by mystery, a black box of technical complexity, the realm of computer programmers or nerdy Excel wizards; but in reality they are not complicated. They are quite simply a set of instructions, the maths that enable computers to solve a problem or complete a task; control driverless cars, compose music or decide which adverts are seen on your social media. Tool such as decision trees, statistical models, neural nets, regression techniques and Bayesian models are all algorithms.

In our age of big data, they are also incredibly powerful control mechanisms deciding what information we are shown on internet search engines, screening job applicants and determining credit ratings. The majority of stock market movements around the world are via algorithm trading, the Internet of Things is powered by algorithms and supply chain logistics are being revolutionised by machine learning (programming that enables computers to adapt and learn from ongoing data analysis rather than follow one set of rules).

It's not uncommon to hear IT auditors say that they will audit up to and around the 'box' but not through it, meaning that the technical 'how' of the computer system turning input into output is 'trusted'. Is this still acceptable? Has the time not come for algorithm auditing to be as commonplace as their use?



Source: Managing algorithmic risk, Deloitte

Are they auditable?

For now, there is a distinction between 'explainable' or 'transparent' algorithms/artificial intelligence and the complexities of black box thinking associated with machine learning. If we focus on the former, explainable and transparent equals auditable.

Your organisation may use thousands of algorithms; it's about taking a risk-based approach.

- Do outputs directly influence material organisational decisions?
- Do outputs become inputs into processes that influence material organisational decisions?
- Are the 'rules' complex, possibly involving artificial intelligence/machine learning?
- How often does an algorithm make a decision?
- Could errors lead to financial misstatement?
- Could errors lead to reputational damage?

Internal auditors recognise the importance of identifying and assuring business critical spreadsheets and modelling tools. Algorithms are no different. They are also the backbone of data analytics, an essential tool in modern auditing.

One aspect of GDPR gives individuals the right to challenge solely automated decisions, such as profiling, being rejected for a loan or issued a warning for repeatedly clocking in late. Audit leaders should consider the provision of assurance against such systems, including the algorithms themselves.

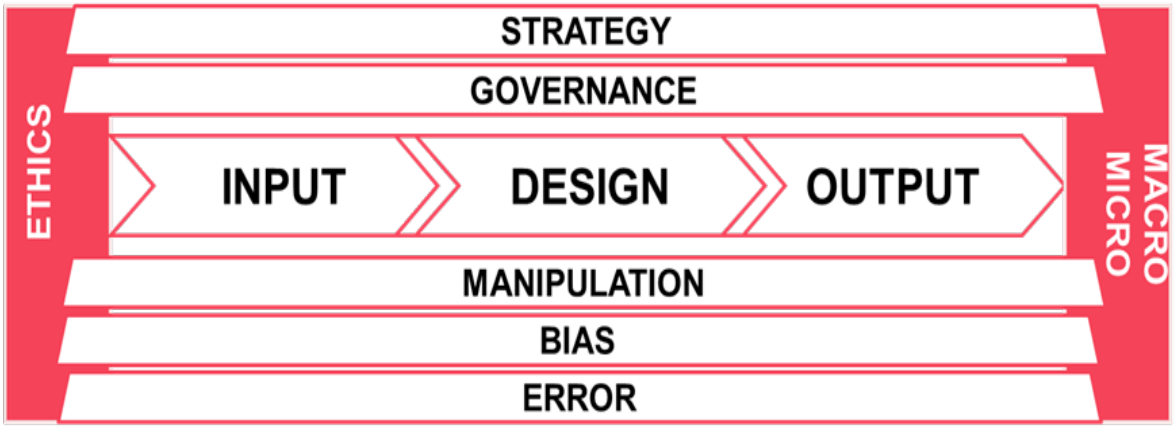
The regulations infer that human intervention reduces the risk of error although this is hotly debated and reflects the societal challenges of our new digital age. There is every possibility that the acceleration of artificial intelligence could lead to new regulations, whilst this is hypothetical, what assurances should the audit committee be thinking about now? As audit leaders should you be raising this topic for discussion?

Audit framework

There is the macro perspective looking a governing principles, policies, authorities and limitations, strategic intent, organisational capability etc. Without structure it is probable that risks could be taken in excess of what the board is willing to accept.

Conversely, there is the micro level detail, providing assurance for specific algorithms. The relevance and accuracy of data inputs, the design of the algorithm itself, interfaces with other systems and the reliability of the eventual output.

Basic Framework for Auditing Algorithms



Strategy

The extent to which the organisation takes advantage of or relies upon complex algorithms should be a strategic one. Pressure for efficiency makes system-driven decision making very attractive. Does the board understand algorithmic risk? Does the organisation understand how to manage it? Subject matter experts must ensure that the board is fully aware of changes to the organisations risk profile.

The opportunities and risks are demonstrated by three examples.

- a major NHS project aiming to improve patient care and waiting times through the use of artificial intelligence with the potential to replace trained specialists
- some councils are exploring big data analysis to predict child abuse to support case workers
- M&S replacing switchboard operators with chatbots in their call centres

Do the capabilities of the organisation match the strategy? There are risks involved in delaying strategy while upskilling employees, likewise there is a risk of over-reliance if partnerships are formed with third parties or specific individuals are relied on.

Governance

Roles and accountabilities will be an essential element of governance as algorithms can form part of end-user computing. IT functions often exclude this from their remit. Does this work for your new control environment or is it time to rewrite the rule book?

It is important to limit the authority of individuals to expose the organisation to digital risk, just as it exists for financial risk. What could this look like?

And then there is the question of ethics, the important question that internal audit and risk professionals should always ensure is being asked; just because we can does it mean we should?

Inputs

The quality of the data being input into an algorithm is critical. Internal audit are expert at providing assurance over the fundamentals of data management including system interfaces for data sources, downtime and recovery.

Design

The algorithmic instructions are paramount. Written by people they are prone to error, bias and manipulation. Basic errors need to be identified. How will this level of assurance be provided? Should it be part of the 2nd line of defence?

Manipulation including fraud is multi-layered, traditional network security controls are paramount and additional consideration may need to be given to preventing and detecting intentional employee sabotage. Minor manipulation/adjustments could erode competitive advantage or reputation as organisations rely heavily on outputs for critical decisions.

It may seem overwhelming but it's achievable; utilise a guest auditor from IT to partner on audits, train the team to understand the basics of coding/programming or co-source the 'techie' element. Audit leaders should be familiar with these skills as they are essential for data analytics.

Overcoming human bias to eliminate discrimination is a major benefit of computer based decision making. However, it is also a significant risk in the design of algorithm itself as it is created by people. And we don't always recognise our own biases to be able to avoid them. Unintended consequences could arise for instance from undue weighting on historic data to predict future high performers in an industry with gender imbalance.

This links back to assurances on the source data, particularly its relevance; challenging the use of appropriate data and data sets. A recruitment organisation called Pymetrics has created a tool to detect bias in algorithms which can also be adapted for other purposes. It is open-source and available for download on Github.

Output

When determining algorithmic risk, a key factor is whether the system-decision is acted on without human intervention and the potential impact of erroneous results.

Internal audit should have awareness of monitoring and validation processes as a minimum. Depending on the depth of digital risk and the use of algorithms, audit leaders should think about any potential gaps in the second line of defence and whether technology is adequately covered.

In 2016 Microsoft launched a social experiment, Tay, a chatbot with machine learning capabilities. It was taken off-line within less than a day because its programmed personality was corrupted by interacting with humans. An extreme example yet one that demonstrates the importance of monitoring for unintended consequences.

Getting Started

Audit leaders know the challenge of creating a comprehensive audit plan, balancing risks and concerns with resource capability and availability. An almost impossible task before adding countless algorithms into the mix!

As with the earlier ethical consideration of using advanced algorithms, the same question also applies to internal auditing, 'just because we can does it mean we should?'

First steps may be consultancy in nature rather than assurance; understanding the risk profile, educating stakeholders, leveraging subject matter experts, exploring capabilities and strategic intent.

Why scare the audit committee over something that sounds 'exciting and new' in the world of internal audit but isn't particularly relevant to the organisation.
Conversely, the digital journey may be accelerating at pace. How well have the algorithmic risks been identified and addressed, does the organisation know its critical algorithmic assets? A governance audit or assurance for an individual algorithm may be appropriate.

Some internal audit functions have standard areas that are included in all engagements to enable ongoing thematic review, such as business continuity, fraud, corporate values; perhaps algorithmic risk management is something to consider adding to this.

Closing Thoughts

Algorithms are not created in isolation; they are part of a wider purpose, an objective being achieved, a problem being solved. They are one element of an integrated solution, process or decision. They enable real-time auditing with the potential to make many traditional audits on the plan obsolete.

Internal audit is a vital part of the digital era, taking a leading role as society adapts to rapid technological advances and the world of automated decisions and interactions. Internal audit has the capability to provide assurance on the fairness and transparency of such decisions.

> *The cause is hidden; the effect is visible to all*
> *Ovid, Roman Poet*

Useful reading

Explainable AI: Driving business value through greater understanding

Managing algorithmic risks

A book called Weapons of Math Destruction by Cathy O'Neil, which can be purchased here.